IN THE UNITED STATES PATENT & TRADEMARK OFFICE

In re application of   :   November 17, 2000

M. Lamberton, et al.   :   IBM Corporation

                                          :   Dept. T81/ 062

Filed: herewith   :   P.O. Box 12195

For: Methods and System for   :   3039 Cornwallis Road

Defeating TCP SYN Flooding Attacks   :   Res. Tri. Park, NC 27709

Preliminary Amendment

Assistant Commissioner for Patents

Washington DC 20231

Sir,

      A preliminary amendment is being provided to the above mentioned case in order to place the case in proper form and idiomatic English for prosecution before the United States Patent and Trademark Office. There is no new content provided by this amendment. Since there are brackets as a portion of the claim, a double bracket is being used to indicate the deletion of those brackets. All elements in the claims that contain brackets are being deleted.

In the Specification:

Page 2, line 13: Please change "mechanism exploits" to --mechanisms exploit--;

      line 22: Please insert --may-- between "system" and "simply";

line 36: Please change "has often" to --often has--.

Page 3, line 12: Please insert --the-- after "Thus,";

line 17: Please insert --attacks-- after "DdoS".

Page 4, line 1: Please insert --the-- between "until" and "attack" and please insert --the-- between "Moreover," and "attack";

line 3: Please change "need" to --needs--.

Page 5, line 6: Please change "this" to --the--;

line 10: Please change "Server" to --The server--;

line 13: Please insert --the-- before "ACK";

line 13 & 14: Please change "If passing checking, ISR" to --If checking is passed, the ISR--;

line 16: Please delete the third "the";

line 20: Please insert --the present-- before "invention".

Page 6, Figure 1: Please change "an half-open" to --a half-open--;

Figure 2-b: Please insert --a-- before "standard";

Figure 4-a: Please change "in server" to --in a server--;

Figure 4-b: Please change "in server" to --in a server--;

Figure 6-b: Please change "computer ISR" to --compute an ISR--;

Figure 6-c: Please change "check ISR" to --check an ISR--.

Page 7, line 14: Please inert --the-- before "server";

line 15: Please insert --the-- before "server";

line 16: Please insert --a-- before "SYN-ACK".

Page 8, line 8: Please insert --may-- between "system" and "simply";

line 25: Please change "Not only the state machine of figure 2 is used" to -- Not only is the state machine of figure 2 used--.

Page 9, line 7: Please insert --the-- before "TCP" and --A-- before "F.M.";

line 10: Please insert --the-- before "server";

line 12: Please insert --the-- after "because";

line 13: Please insert --the-- before "F.M.";

line 15: Please insert --the-- before "TCB";

FR920000023US1

line 18: Please insert --the-- before "F.M.";

line 20: Please change "move" to --moves--;

line 21: Please change "close" to --closes--;

line 22: Please insert --the-- before "F.M.";

line 24: Please insert --the-- before "SYN";

line 30: Please change "connection" to --connections--;

line 31: Please change "to" to --for--;

line 36: Please insert --a-- before "TCP F.M." and insert --attacks-- after "DoS".

Page 10, line 3: Please insert --the-- before "F.M.";

line 7: Please change "into" to --in-- and insert --the-- before process;

line 10: Please change "a ACK" to --an ACK--;

line 12: Please insert --the-- before "server";

line 16: Please change "a ACK" to --an ACK--;

line 35: Please insert --the-- before "target".

Page 11, line 4: Please insert --the-- before "TCP" and please insert change "Header" to --The header--;

line 5: Please change "a ACK" to --an ACK--;

line 6: Please insert --the-- after "only";

line 8: Please insert --an-- before "ISR";

line 10: Please insert --the-- before the first "ISR";

line 11: Please insert --the-- before "server";

line 12: Please insert --the-- before "ISR";

line 14: Please insert --ISR-- after "quasi-unaltered" and change "except" to --expects--;

line 15: Please insert --the-- before "client" and insert --a-- before "field";

line 23: Please delete "of";

line 33: Please insert --the-- before "server".

Page 12, line 1: Please insert --the-- before "next";

line 3: Please insert --an-- before "ISR";

line 4: Please insert --the-- before "following";

FR920000023US1

line 7: Please insert --a-- before "SYN-ACK" and --an-- before "ISS";

line 9: Please change "unique" to --uniquely--;

line 10: Please insert --a-- before "SYN";

line 15: Please insert --the-- before "server";

line 17: Please change "a ACK" to --an ACK--;

line 18: Please change "Server is" to --The server is--;

line 25: Please insert --the-- before "next" and change "in checking ISR" to --of checking the ISR--;

line 27: Please insert --an-- before "ISR ACK";

line 29/30: Please change "ACK is dropped [423] and process resume" to --the ACK is dropped [423] and processing is resumed--;

line 32: Please insert --the-- before "ISR";

line 35: Please insert --the-- before "server";

line 36: Please delete "to" .

Page 13, line 1 : Please change "derive from ISR" to --derivation from the ISR--;

line 2: Please insert --the-- before "next" and change "in" to --of--;

line 5: Please insert --the-- before "ISR";

line 5/6: Please change "At completion of it TCB" to --At completion, the TCB--;

line 6: Please insert --the-- before "state";

line 11: Please insert --an-- before "ISR" and --a-- in front of "server";

line 12: Please insert --the-- before "server";

line 15: Please delete "a" after "received";

line 16: Please change "An abundant" to --Abundant--;

line 25: Please change "key" to --keys--;

line 29: Please change "derive current" to --derive the currently--;

line 30: Please insert --the-- before "PRN";

line 31: Please insert --the-- before "key".

Page 14, line 9 : Please change "Server" to --The server--;

line 12: After "example" please insert --, the--;

line 24: Please insert --the-- before "server";

FR920000023US1

line 35: Please insert --the-- before "server".

Page 15, line 8: Please insert --the-- before "signature";

line 16: Please insert --a-- after "if";

line 23: Please change "as" to --that--;

line 24: Please insert --the-- before "former";

Page 16, line 3: Please insert --the-- before "server" and insert --the-- before "global";

line 4: Please insert --the-- before "client";

line 6: Please insert --the-- before the first "client" and please change "Server" to --The server--;

line 7: Please insert --the-- before "server" and insert --the-- before "TCP";

line 8: Please insert --the-- before "current" and insert --the-- before "PRN";

line 20: Please change "Checking" to --The checking--;

line 21: Please insert --an-- before "ISR";

line 22: Please replace "are got. The" with --, the--;

line 23: Please change "Selected" to --The selected--;

line 25: Please insert --the-- before "server";

line 27: Please insert --the-- before "ISR";

line 30: Please insert --the-- before "signature";

line 31: Please insert --the-- before "category";

line 32: Please change "to" to --with--.

Page 17, line 1: Please insert --the-- after "however";

line 3: Please inert --the-- before "answer";

line 5: Please insert --the-- before "former";

line 8: Please insert --the-- before "comparison" and insert --the-- before "answer";

line 16: Please insert --be-- after "could";

line 18: Please change ". In which" to --, in which--.

In the claims:

1   1 (Once Amended). A method for defeating, in a server unit [[110]] of an IP (Internet

2   Protocol) network [[105]], a SYN flooding attack, said server unit running TCP

3   (Transport Control Protocol) to allow the establishment of one or more TCP connections

4   [[102]] with one or more client units [[100]], said method comprising the steps of:

5   upon having activated TCP [[400]] in said server unit:

6   listening [[410, 412]] for the [receiving] receipt of a SYN message sent [[120]]

7   from one said client unit [[100]];

8   upon receiving [[414] a] said SYN message:

9   computing [[420]] an ISR (Initial Sequence number Receiver side) [[131]];

10   responding [[430]] to said client unit [[100]] with a SYN-ACK message [[130]]

11   including said computed said ISR:

12   resuming [[432]] to said listening step.

1   Claim 2 (once amended). The method according to claim 1 wherein the step of

2   computing said ISR further includes the steps of:

3   concatenating a randomly generated key [[500]] with an identification of one said

4   TCP connection said identification including:

5   a client socket [[510]] and a server socket [[520]];

6   hashing [[530]] said concatenation, thus obtaining a server signature [[540]];

7   concatenating said server signature and a category index [[550]] referring to a

8   set of predefined TCP connection categories [[570]];

9   thereby, obtaining a computed ISR [[550]].

1   Claim 3 (once amended). The method according to [any one of the previous claims]

2   claim 1 or 2 wherein said computing step further comprises the steps of:

3   [keep] updating [[602]], in said server unit [[110], a pseudo-random number

4   (PRN) generator [[600]];

5   holding a current key [[604]];

6   remembering a former key [[606]]; and

7   using said current key [[616]] as said randomly generated key [[500]] for said

8   computed ISR.

1   Claim 4 (once amended). The method according to [any one of the previous claims]

2   claim 2 wherein the step of concatenating said category index includes the further step

3   of:

4   picking up a category index [[618]] within said set of predefined connection

5   categories [[570]] on the basis of the content of said received [said] SYN message

6   [[610]].

1   Claim 5 (once amended). The method according to [any one of the previous claims]

2   claim 3 wherein said updating step includes the step of:

3   [keep] updating said PRN generator [[600]] at a rate not higher than [the] an MSL

4   (Maximum Segment Lifetime) defined in said TCP connection.

Claim 6 (once amended). A method for defeating, in [said] a client unit [[100]] of an IP

network [[105]], a SYN flooding attack, said method comprising the steps of:

        upon receiving [[132]] [said] a SYN-ACK message from [said] a server unit

[[110]]:

                normally responding with an ACK message [[140]], said step of normally

responding comprising the step of:

                including, in said ACK message [[140]], [said] a computed ISR [[420, 555]]

incremented by one; [thereby, complying with the regular TCP rules].

1   Claim 7 (once amended). A method for defeating, in [said] a server unit [[110]] of [said]

2   an IP network [[105]] having a TCP connection, [said] a SYN flooding attack, said

3   method comprising the steps of:

4   upon having activated TCP in said server unit:

5   listening [[411,413]] for the receiving of [a said] an ACK message sent [[140]]

6   from one [said] client unit[[100]];

7   upon receiving [[415]] [a] said ACK message:

8   checking [[421] said] an ISR;

9   if failing said checking step:

10   dropping [[423]] said ACK message;

11   if passing said checking step:

12   decoding [[425]] said ISR as being an authentic [said] computed ISR;

13   allocating resources [[427]] for [a] said TCP connection according to

14   content of said computed ISR;

15   establishing [[429]] [a] said TCP connection;

16   in either case:

17   resuming [[431] to] said listening step [[411]].

1   Claim 8 (once amended). The method of claim 7 wherein the decoding step includes

2   the step of :

3   interpreting [said]_a category index [[550]] extracted [[688]] from said computed

4   ISR [[555]].

Claim 9 (once amended). The method according to [any of claim 7 or] claim 8 wherein

the allocating step includes the step of:

     selecting a predefined set of parameters, for said TCP connection, on the basis

of the value of said category index [[550]].

Claim 10. The method according to claim 7 wherein the step of checking said ISR

2   includes, upon receiving said ACK message [[670]], the steps of:

3   having, firstly, selected said current key [[678]]:

4   getting said selected key [[676]];

5   concatenating said selected key with an identification of said TCP connection,

6   said identification including:

7   a client socket [[672]] and a server socket [[674]];

8   hashing [[682]] said concatenation, thus [,] obtaining a re-computed server

9   signature [[684]];

10   extracting [[690]] an acknowledgment field [[562]] from said ACK message;

11   decrementing [[692]] content of said acknowledgment field;

12   extracting said server signature [[694]];

13   comparing [[686]] said re-computed server signature [[684]] and said extracted

14   [said] server signature [[694]];

15   if said extracted server signature and said re-computed server signature match

16   [matching]:

17   extracting [[688]] said category index; [thus, passing checking]

18   if said extracted server signature and said re-computed server signature to not

19   match [failing]:

20   checking if a second loop status [[696]] is set;

21   If not set:

22   selecting [said] a former key [[698]];

23   setting [said] a second loop status [[679]];

24   resuming execution at said [above] getting step [[676]];

25   if set:

26   failing said checking step.

Please cancel claims 11, 12 and 13 without prejudice.

Claim 14 (new). A computer program product for defeating, in a server unit of an IP (Internet Protocol) network , a SYN flooding attack, said server unit running TCP (Transport Control Protocol) to allow the establishment of one or more TCP connections with one or more client units, said computer program product having computer readable program code comprising the steps of:

upon having activated TCP in said server unit:

computer readable program code for listening for the receipt of a SYN message sent from one said client unit;

upon receiving said SYN message:

computer readable program code for computing an ISR (Initial Sequence number Receiver side) ;

12   computer readable program code for responding to said client unit with a SYN-

13 ACK message including said computed said ISR:

14   computer readable program code for resuming said listening step.

1 Claim 15 (new). The computer program product according to claim 14 wherein the step

2 of computing said ISR further includes the steps of:

3   computer readable program code for concatenating a randomly generated key

4 with an identification of one said TCP connection said identification including:

5   a client socket and a server socket;

6   computer readable program code for hashing said concatenation, thus obtaining

7 a server signature;

8   computer readable program code for concatenating said server signature and a

9 category index referring to a set of predefined TCP connection categories ;

10   thereby, obtaining a computed ISR .

Claim 16 (new). The computer program product according to claim 14 or 15 wherein

said computing step further comprises the steps of:

   computer readable program code means for updating, in said server unit, a

pseudo-random number (PRN) generator;

   computer readable program code for holding a current key;

   computer readable program code for remembering a former key; and

7   computer readable program code for using said current key as said randomly

8 generated key for said computed ISR.

1 Claim 17 (new) . A system for implementing a shield for defeating TCP SYN flooding

2 attacks said system comprising:

3   an IP (Internet Protocol) network;

4   a server unit running TCP (Transportation Control Protocol) to allow the

5 establishment of one or more TCP connections; and

6   one or more client units; wherein, once said TCP is activated in said server unit,

7   said server unit listens for the receipt of a SYN message from one or more of said client

8   units; and whereupon receiving said SYN message, said server unit computes an ISR

9   (Initial Sequence number Receiver side), responds to said client unit with a SYN-ACK

10   message including said computed ISR and resumes listening for further SYN

11   messages.

Remarks

Claims 1-10 and 14-17 are presented for examination. Claims 11, 12 and 13 have been canceled, claims 1-10 have been amended and claims 14-17 are new to the application. The Applicant's apologize for the number of amendments presented, but have only been given an image of the application hence are unable to easily provide a clean copy. The Applicant's have made a good faith effort to place the Application in condition for allowance. It is respectfully requested that the Examiner proceed to allow the case at an early date.

Respectfully submitted,

Jeanine S. Ray-Yarletts
Attorney for Applicant
Reg. No. 39,808

JSR:jdl
Docket No: FR9-2000-0023-US1
Phone: (919) 543-2541 ;Fax: (919) 254-4330.

FR920000023US1